VPN IPSec Windows 2000 – Zywall 10, 50, 100



Zywall 10, 50, 100 IPSec Setup Menu (letzte Rule editieren/ éditez le dernier Rule)

| 🖾 C:\WINNT\System32\cmd.exe - telnet 192.168.1.1 | |
|--|----------|
| Menu 27.1.1 - IPSec Setup Index #= 120 Name= Dynamic Active= Yes | |
| My IP Addr= 195.246.70.100 Secure Gateway IP Addr= 0.0.0.0 Protocol= 0 Local: IP Addr Start= 192.168.1.0 Port Start= 0 Remote: IP Addr Start= N/A Port Start= N/A Port Start= N/A Enable Replay Detection= No Key Management= IKE Edit IKE Setup= No Edit Manual Setup= N/A | |
| Press ENTER to Confirm or ESC to Cancel: Press Space Bar to Toggle. | _ |

"Edit IKE Setup = YES" Menu



Windows 2000



| 🛃 Lokale Sicherheitseinstellungen | | | | | | | |
|--|--|--|------------------------------|--|--|--|--|
| Vorgang Ansicht ← → 🛍 🖬 🕼 🛱 😫 🏠 🏪 | | | | | | | |
| Struktur | Name 🛆 | Beschreibung | Richtlinie zugewiesen | | | | |
| Sicherheitseinstellungen Contrichtlinien Contrichtlinien Contrichtlinien öffentlicher Schlüssel Contrict IP-Sicherheitsrichtlinie erstellen IP-Filterlisten und Filter stellen IP-Filterlisten und Filter stellen IP-Filterlisten und Filter stellen IP-Sicherheitsrichtlinie Alle Tasks Ansicht Aktualisieren Liste exportieren Hilfedatei anzeigen | Anne Antwort) Client (nur Antwort) Server (Sicherheit anf Sicherer Server (Siche | Normale (ungesicherte) Kom Sicherheit ist für den gesam Sicherheit ist für den gesam | Nein Nein Nein Nein | | | | |
| Erstellt eine IP-Sicherheitsrichtlinie. | | | | | | | |

| Assistent für IP-Sicherheitsrichtlinien | ? × |
|--|-----------|
| IP-Sicherheitsrichtlinienname Benennen Sie die Sicherheitsrichtlinie und geben Sie optional eine kurze Beschreibung ein. | Ē |
| Name: Zywall Beschreibung: | |
| | × |
| | |
| <zurück weiter=""></zurück> | Abbrechen |

| Assistent für IP-Sicherheitsrichtlinien | ?× |
|--|------|
| Anforderungen für sichere Kommunikation Geben Sie an, wie diese Richtlinie auf Anforderungen betreffend sicherer Kommunikation, antwortet. | Ē |
| Die Standardantwortregel wird für Sicherheitsanforderungen von Remotecomputern verwendet, falls keine andere Regel angewendet wird. Für sichere Kommunikation muss der Computer auf Anforderungen betreffend sicherer Kommunikation antworten. | |
| Die Standardantwortregel aktivieren | |
| \triangleright | |
| | |
| | |
| | |
| | |
| < Zurück Weiter > Abbre | chen |



| Eigenschaften von Zywall | ? × |
|--|-------------|
| Regeln Allgemein | |
| Sicherheitsregeln für die Kommunikation mit anderen Comp | outern |
| IP-Sicherheitsregeln: | |
| IP-Filterliste Filteraktion Authentifizieru | Tu |
| Comparison Standardantwort Kerberos | Ke |
| International Assistant verv | ▶ venden |
| OK Abbr | rechen |



| Sicherheitsregel-Assistent | ? × |
|---|-----------------|
| Tunnelendpunkt Der Tunnelendpunkt ist der dem Ziel des IP-Verkehrs nächste Tunnelcomputer, entsprechend der Spezifikation durch die IP-Filterliste der Sicherheitsregel. | Ē |
| Ein IPSec-Tunnel ermöglicht Paketen das Durchqueren eines öffentlichen oder priv Netzwerks auf der Sicherheitsstufe einer direkten Verbindung zwischen zwei Comp | /aten utern. |
| Geben Sie Tunnelendpunkt für die IP-Sicherheitsregel an: | |
| O Diese Regel spezifiziert keinen Tunnel | |
| Oer Tunnelendpunkt wird durch diese IP-Adresse spezifiziert: | |
| 195 . 246 . 70 . 100 | |
| <zurück weiter=""> At</zurück> | obrechen |

| Sicherheitsregel-Assistent | | ?× |
|---|---------------------------|-----------|
| Netzwerktyp Die Sicherheitsregel muss auf einen Netzwe | erktyp angewendet werden. | <u>I</u> |
| Wählen Sie den Netzwerktyp: | | |
| Alle Netzwerkverbindungen LAN RAS | | |
| | < Zurück Weiter > | Abbrechen |

| Assistent für IP-Sicherheitsrichtlinien | ? × |
|---|----------|
| Authentifizierungsmethode Bearbeiten Sie die Sicherheitsregel, nachdem der Assistent fertig gestellt wurde, um mehrere Authentifizierungsmethoden hinzuzufügen. | 圓 |
| Legen Sie die ursprüngliche Authentifizierungsmethode für diese Sicherheitsregel fest: | |
| O Windows 2000-Standard (Kerberos V5-Protokoll) | |
| O Verwenden eines Zertifikats von dieser Zertifizierungsstelle: | |
| Durchsuchen. | |
| Diese Zeichenkette zum Schutz des Schlüsselaustauschs verwenden: | _ |
| zyxelzywall | <u>-</u> |
| | |
| < Zurück Weiter > Abbi | rechen |

| herheitsregel-Assistent | | <u>? ×</u> |
|---|--|-------------------|
| IP-Filterliste Wählen Sie die IP-Filterliste für der angewendet werden soll. | n IP-Verkehrstyp für den diese Rege | Ē |
| Klicken Sie auf "Hinzufügen", um folgenden Liste den Anforderunger IP-Filterlisten: | ein neues Filter zu erstellen, wenn k n entspricht. | ein Filter in der |
| Name | Beschreibung | Hinzufijgen |
| All ICMP-Verkehr | Passt alle ICMP-Pakete zwisc | |
| O Gesamter IP-Verkehr | Passt alle IP-Pakete von dies | Bearbeiten |
| | | Entfernen |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | < Zurück Weite | r > Abbrechen |

| 👷 IP-Filte | rliste | | | ? × |
|------------|--|---|--|--------------------------|
| Tata | Eine IP-Filterliste beste Subnetze, IP-Adresser | ht aus mehreren Filt i und Protokolle zu i | ern. Dadurch können v einem IP-Filter kombinier | erschiedene t werden. |
| Name: | | | | |
| Neue IF | P-Filterliste | | | |
| Beschrei | ibung: | | | Hinzufügen |
| | | | <u></u> | Bearbeiten |
| | | | v | Entfernen |
| Filter: | | | 🔽 Assi | istent verwenden |
| Gespi | . Beschreibung | Protokoll | Quellport | Zielport |
| | | | | |
| • | | | | Þ |
| | | | OK | Abbrechen |

| Filter-Assistent | <u>? ×</u> |
|--|-------------------------|
| Quelle des IP-Verkehrs Legen Sie die Quelladresse des IP-Verkehrs fest. | E |
| Quelladresse: Eigene IP-Adresse | |
| < Zur | iück Weiter > Abbrechen |

| Filter-Assistent | | | | | | | | | ? × |
|---|-----------|-------|---------|----|-------|---|-------|-----|-----------|
| Ziel des IP-Verkehrs Legen Sie die Zieladresse | des IP-Ve | rkehr | s fest. | | | | | | Ē |
| Zieladresse: | | | | | | | | | |
| Spezielles IP-Subnetz | | | | | | • | | | |
| IP-Adresse: | 192 | . 1 | 68 | • | 1 | • | 0 | | |
| Subnetzmaske: | 255 | . 2 | 255 | | 255 | • | 0 | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | ×Z | urück | | Weite | ı>₽ | Abbrechen |

| Filter-Assistent | ? × |
|---|--------|
| Typ des IP-Protokolls Legen Sie den IP-Protokolltyp fest. Wenn dieser Typ IP-Ports unterstützt, müssen Sie auch einen IP-Port angeben. | Ē |
| Wählen Sie einen Protokolltyp: Beliebig | |
| | |
| | |
| | |
| | |
| < Zurück Weiter > Abb | rechen |



| 🐮 IP-Filte | rliste | | | ? × |
|------------|---|---|---|-----------------------|
| | Eine IP-Filterliste besteł Subnetze, IP-Adressen | it aus mehreren Filtern. I und Protokolle zu einen | Dadurch können ve n IP-Filter kombiniert | rschiedene werden. |
| Name: | | | | |
| W2K to 2 | Zywall | | | |
| Beschreit | oung: | | | Hinzufügen |
| | | | <u> </u> | Bearbeiten |
| | | | v | Entfernen |
| Filter: | | | 🔽 Assis | tent verwenden |
| Gespi | Beschreibung | Protokoll | Quellport | Zielport |
| Ja | | beliebig(e) | beliebig(e) | beliebig(e) |
| | | | | |
| • | | | | Þ |
| | | | Schließer | Abbrechen |

| Sicherheitsregel-Assistent | | <u>?</u> × |
|--|---|-------------------------|
| IP-Filterliste Wählen Sie die IP-Filterliste für der angewendet werden soll. | n IP-Verkehrstyp für den diese Rege | Ĩ |
| Klicken Sie auf "Hinzufügen", um folgenden Liste den Anforderunge IP-Filterlisten: | ein neues Filter zu erstellen, wenn k n entspricht. | ein Filter in der |
| Name | Beschreibung | Hinzufügen |
| All ICMP-Verkehr Gesamter IP-Verkehr W2K to Zywall | Passt alle ICMP-Pakete zwisc Passt alle IP-Pakete von dies | Bearbeiten Entfernen |
| | < Zurück Weite | r> |

| Sicherheitsregel-Assistent | | ? × |
|---|--|---|
| Filteraktion Wählen Sie die Filteraktion für diese | e Sicherheitsregel. | 圓 |
| Klicken Sie auf "Hinzufügen", um e folgenden Liste den Anforderungen um eine Filteraktion Schritt für Schri | ine neue Filteraktion zu erstellen, v entspricht. Aktivieren Sie "Assiste tt zu erstellen. | wenn keine in der nt verwenden'', Assistent verwenden |
| Filteraktionen: | | |
| O Sicherheit anfordern (optional) O Sicherheit erforderlich O Zulassen | Ungesicherte Kommunikation Ungesicherte Kommunikation Ungesicherte IP-Pakete durc | Bearbeiten |
| | < Zurück Weite | er > Abbrechen |

| Filteraktions-Assistent | ? × |
|---|---------|
| Name der Filteraktion Benennen Sie diese Filteraktion und geben Sie optional eine kurze Beschreibung ein. | E. |
| Name: | |
| Beschreibung: | |
| | X |
| | |
| < Zurück Weiter > 📐 Ab | brechen |

| Filteraktion | | | ? × |
|--|----------|----------|-----------|
| Allgemeine Optionen der Filteraktion Legen Sie das Filteraktionsverhalten fest. | | | 163 |
| O Zulassen | | | |
| C Sperren | | | |
| Sicherheit aushandeln: | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | < Zurück | Weiter > | Abbrechen |

| Filteraktions-Assistent |
|--|
| Kommunikation mit Computern, die kein IPSec unterstützen Die Kommunikation mit Computern, die kein IPSec unterstützen, stellt ein Sicherheitsrisiko für das Netzwerk dar. |
| Soll Kommunikation mit anderen Hosts zugelassen werden, die IPSec nicht unterstützen? |
| Keine Kommunikation mit Computern zulassen, die IPSec nicht unterstützen |
| O Auf unsichere Kommunikation zurückgreifen |
| Verwenden Sie diese Option für Computer, die kein IPSec unterstützen. Die Kommunikation mit Computer, die kein IPSec unterstützen, stellt ein Sicherheitsrisiko im Netzwerk dar. |
| < Zurück Weiter > Abbrechen |

| Sicherheitsmethoden-Assistent | ? × |
|---|-----------|
| Sicherheit des IP-Verkehrs Geben Sie die Sicherheitsmethode für den IP-Verkehr an. Bearbeiten Sie die Filteraktion, nachdem der Assistent fertig gestellt wurde, um mehrere Sicherheitsmethoden hinzuzufügen. | 167 |
| Diese Filteraktion erfordert mindestens eine Sicherheitsmethode für IP-Verkehr. | |
| Hoch (Encapsulated Secure Payload) Daten werden verschlüsselt, authentifiziert und nicht geändert. Mittel (Authenticated Header) Daten werden authentifiziert und nicht geändert, aber nicht verschlüsselt. Benutzerdefiniert | |
| < Zurück Weiter > | Abbrechen |

| Einstellungen der Sicherheitsmethoden anpassen 🛛 🤶 🗙 |
|---|
| Legen Sie die Einstellungen für die benutzerdefinierte Sicherheitsmethode fest. |
| Daten- und Adressintegrität ohne Verschlüsselung (AH): Integritätsalgorithmus: |
| MD5 |
| Datenintegrität und Verschlüsselung (ESP): |
| Integritätsalgorithmus: |
| MD5 |
| Verschlüsselungsalgorithmus: |
| DES |
| Sitzungsschlüsseleinstellungen: |
| ■ Neuen Schlüssel alle: Veuen Schlüssel alle: |
| 100000KBytes generieren9600Sekunden generieren |
| |
| OK Abbrechen |

| Sicherheitsmethoden-Assistent | ? × |
|--|-----------|
| Sicherheit des IP-Verkehrs Geben Sie die Sicherheitsmethode für den IP-Verkehr an. Bearbeiten Sie die Filteraktion, nachdem der Assistent fertig gestellt wurde, um mehrere Sicherheitsmethoden hinzuzufügen. | 100 |
| Diese Filteraktion erfordert mindestens eine Sicherheitsmethode für IP-Verkehr. | |
| Hoch (Encapsulated Secure Payload) Daten werden verschlüsselt, authentifiziert und nicht geändert. Mittel (Authenticated Header) Daten werden authentifiziert und nicht geändert, aber nicht verschlüsselt. | |
| Benutzerdefiniert Einstellungen | |
| | |
| < Zurück Weiter > | Abbrechen |



| Eigenschaften von IKE | ? × |
|---|-------------------------|
| Sicherheitsmethoden Allgemein | |
| Zulassen Sperren Sicherheit aushandeln: Beihenfolge der Sicherheitsmethoden: | |
| Typ AH-Integrität ESP-Vertraulich ES | Hinzufügen _s |
| Benutze <keine> DES ME</keine> | Bearbeiten |
| | Entfernen |
| | Nach oben |
| T D | Nach unten |
| Unsichere Kommunikat, annehmen, aber immer mit IPSe | c antworten |
| 🔲 Unsichere Komm. mit Computern zulassen, die IPSec nic | cht unterstützen |
| Sitzungsschlüssel mit Perfect Forward Secrecy (PFS) | |
| OK Abbrechen | Übernehmen |

| Sicherheitsmethode ändern |
|---|
| Sicherheitsmethode |
| Hoch (ESP) Daten werden verschlüsselt, authentifiziert und nicht geändert. |
| Mittel (AH) Daten werden authentifiziert und weder ge |
| Benutzerdefiniert (nur für erfahrene Benutzer) Einstellungen |
| |
| |
| UK Abbrechen Ubernehmen |

| Neue Sicherheitsmethode |
|--|
| Sicherheitsmethode |
| C Hoch (ESP) |
| Daten werden verschlüsselt, authentifiziert und nicht geändert. |
| C Mittel (AH) |
| Daten werden authentifiziert und weder geändert, noch verschlüsselt. |
| Benutzerdefiniert (nur für erfahrene Benutzer) Einstellungen |
| OK Abbrechen Übernehmen |

| Einstellungen der Sicherheitsmetho | den anpassen ?X |
|--|--|
| Legen Sie die Einstellungen für die benut | zerdefinierte Sicherheitsmethode fest. |
| Daten- und Adressintegrität ohne Ver Integritätsalgorithmus: | rschlüsselung (AH): |
| MD5 💌 | |
| Datenintegrität und Verschlüsselung Integritätsalgorithmus: SHA1 | (ESP): |
| Verschlüsselungsalgorithmus: DES | |
| Sitzungsschlüsseleinstellungen: | Veuen Schligsel alle: |
| 1000000 KBytes generieren | 3600 Sekunden generieren |
| | OK Abbrechen |

| Eigenschafte | n von IKE | | | ? × |
|--|---|--|--------------------------------|----------------------------------|
| Sicherheitsm | ethoden Allgeme | ein | | |
| C Zulasse C Sperrer C Sicherh Reihenfolge | en n leit aushandeln: e der Sicherheitsm | ethoden: | | |
| Тур | AH-Integrität | ESP-Vertraulich | ES | Hinzufügen |
| Benutze | <keine> <keine></keine></keine> | DES | SH | Bearbeiten |
| | | | | Entfernen |
| | | | | Nach oben |
| • | | | ▶ | Nach unten |
| ✓ Unsiche ✓ Unsiche ✓ Unsiche ✓ Sitzung | ere Kommunikat. a ere Komm. mit Con sschlüssel mit Perf | nnehmen, aber imme nputern zulassen, die ect Forward Secrecy | rmit IPSe IPSecnie (PFS) | ec antworten cht unterstützen |
| | | | brechen | Übernehmen |

| Eigenschaften von Neue Regel | <u>? ×</u> |
|--|--|
| Authentifizierungsmethoden Tu IP-Filterliste | nneleinstellungen Verbindungstyp Filteraktion |
| Die gewählte Filteraktic sicherer Netzwerkverke Verkehr gesichert wird. | on spezifiziert, ob mit dieser Regel ehr ausgehandelt wird und wie der |
| Filteraktionen: | |
| Name | Beschreibung |
| ⊙IKE | |
| Sicherheit anfordern (optional) Sicherheit erforderlich Zulassen | Ungesicherte Kommunikation wi Ungesicherte Kommunikation wi Ungesicherte IP-Pakete durchla |
| Hinzufügen Bearbeiten | Entfernen 🔽 Assistent verwenden |
| Schli | eßen Abbrechen Übernehmen |

| Eigenschaften von Zywa | all | | ? X |
|------------------------|----------------------------|--------------------|-------------|
| Regeln Allgemein | | | |
| Sicherheitsre | egeln für die Kommunikatio | n mit anderen Comp | outern |
| IP-Sicherheitsregeln: | | | |
| IP-Filterliste | Filteraktion | Authentifizieru | Tu |
| ☑ W2K to Zywall | IKE | Vorinstallierter | 19 |
| Comparison | Standardantwort | Kerberos | Ke |
| Hinzufügen | peiten | Assistent verv | ▶ venden |
| | S | chließen Abb | rechen |

IP von DFÜ / IP de l'accés à distance = 213.3.123.66

| Status von Bluewin | | <u>? ×</u> |
|---|--|------------|
| Allgemein Details | | 1 |
| Eigenschaft Servertyp Übertragungen Authentifizierung Komprimierung PPP-Multilinkframing Server-IP-Adresse Client-IP-Adresse | Wert PPP TCP/IP MD5 CHAP (keine) Inaktiv 213.3.122.1 213.3.123.66 | |
| | | Schließen |

| Sicherheitsregel-Assistent |
|---|
| Tunnelendpunkt Der Tunnelendpunkt ist der dem Ziel des IP-Verkehrs nächste Tunnelcomputer, entsprechend der Spezifikation durch die IP-Filterliste der Sicherheitsregel. |
| Ein IPSec-Tunnel ermöglicht Paketen das Durchqueren eines öffentlichen oder privaten Netzwerks auf der Sicherheitsstufe einer direkten Verbindung zwischen zwei Computern. |
| Geben Sie Tunnelendpunkt für die IP-Sicherheitsregel an: |
| O Diese Regel spezifiziert keinen Tunnel |
| Der Tunnelendpunkt wird durch diese IP-Adresse spezifiziert: |
| 213 . 3 . 123 . 66 |
| |
| |
| |
| |
| |
| |
| <zurück weiter=""></zurück> |

| Sicherheitsregel-Assistent | <u>? ×</u> |
|--|------------|
| Netzwerktyp Die Sicherheitsregel muss auf einen Netzwerktyp angewendet werden. | Ē |
| Wählen Sie den Netzwerktyp: | |
| C Alle Netzwerkverbindungen ○ LAN ④ RAS | |
| < Zurück Weiter > | Abbrechen |

| Assistent für IP-Sicherheitsrichtlinien | ? × |
|---|---------|
| Authentifizierungsmethode Bearbeiten Sie die Sicherheitsregel, nachdem der Assistent fertig gestellt wurde, um mehrere Authentifizierungsmethoden hinzuzufügen. | Ţ |
| Legen Sie die ursprüngliche Authentifizierungsmethode für diese Sicherheitsregel fes | t |
| Windows 2000-Standard (Kerberos V5-Protokoll) | |
| O Verwenden eines Zertifikats von dieser Zertifizierungsstelle: | |
| Durchsucher | h |
| Diese Zeichenkette zum Schutz des Schlüsselaustauschs verwenden: | |
| zyxelzywal | × |
| | |
| < Zurück Weiter > Abl | prechen |

| IP-Filterliste Wählen Sie die IP-Filterliste für den IP-Verkehrstyp für den diese Regel angewendet werden soll. Klicken Sie auf "Hinzufügen", um ein neues Filter zu erstellen, wenn kein Filter in der folgenden Liste den Anforderungen entspricht. |
|---|
| Klicken Sie auf "Hinzufügen", um ein neues Filter zu erstellen, wenn kein Filter in der folgenden Liste den Anforderungen entspricht. |
| IP-Filterlisten: |
| Name Beschreibung Hinzufügen |
| O All ICMP-Verkeni Passt alle ICMP-Pakete von dies O Gesamter IP-Verkehr Passt alle IP-Pakete von dies O W2K to Zywall Entfernen |
| |

| 🐮 🖥 IP-Filte | rliste | | | ? × |
|--------------|---|---|---|------------------------|
| | Eine IP-Filterliste besteł Subnetze, IP-Adressen | nt aus mehreren Filtern. und Protokolle zu einer | Dadurch können ve n IP-Filter kombiniert | erschiedene werden. |
| Name: | | | | |
| Zywall t | o W2k | | | |
| Beschrei | ibung: | | | Hinzufügen |
| | | | A | Bearbeiten |
| | | | v | Entfernen |
| Filter: | | | 🔽 Assi: | stent verwenden |
| Gespi | . Beschreibung | Protokoll | Quellport | Zielport |
| | | | | |
| | | | OK | Abbrechen |

| ilter-Assistent |
|--|
| Quelle des IP-Verkehrs Legen Sie die Quelladresse des IP-Verkehrs fest. |
| Quelladresse: |
| Spezielles IP-Subnetz |
| IP-Adresse: 192 . 168 . 1 . 0 |
| Subnetzmaske: 255 . 255 . 255 . 0 |
| |
| |
| |
| |
| |
| < Zurück Weiter > Abbrechen |

| Filter-Assistent | <u>?</u> × |
|--|------------|
| Ziel des IP-Verkehrs Legen Sie die Zieladresse des IP-Verkehrs fest. | Ē |
| Zieladresse: Eigene IP-Adresse | |
| < Zurück Weiter > | Abbrechen |

| Filter-Assistent | ? × |
|---|---------|
| Typ des IP-Protokolls Legen Sie den IP-Protokolltyp fest. Wenn dieser Typ IP-Ports unterstützt, müssen Sie auch einen IP-Port angeben. | Ē |
| Wählen Sie einen Protokolltyp: Beliebig 0 | |
| | |
| < Zurück Weiter > 🔀 Abl | brechen |



| 🇱 IP-Filt | erliste | | | <u>? ×</u> |
|-----------|---|---|---|-----------------------|
| | Eine IP-Filterliste besteh Subnetze, IP-Adressen | it aus mehreren Filtern. und Protokolle zu einer | Dadurch können ve m IP-Filter kombiniert | rschiedene werden. |
| Name: | | | | |
| Zywall | to W2k | | | |
| Beschre | eibung: | | | Hinzufügen |
| | | | <u>^</u> | Bearbeiten |
| | | | ~ | Entfernen |
| Filter: | | | 🔽 Assis | tent verwenden |
| Gespi | Beschreibung | Protokoll | Quellport | Zielport |
| Ja | | beliebig(e) | beliebig(e) | beliebig(e) |
| | | - | | |
| | | | | |
| | | | Schließen | Abbrechen |

| Sicherheitsregel-Assistent | | <u>? ×</u> |
|---|---|-------------------------|
| IP-Filterliste Wählen Sie die IP-Filterliste für der angewendet werden soll. | n IP-Verkehrstyp für den diese Rege | Ē |
| Klicken Sie auf "Hinzufügen", um folgenden Liste den Anforderunger IP-Filterlisten: | ein neues Filter zu erstellen, wenn k n entspricht. | ein Filter in der |
| Name | Beschreibung | Hinzufügen |
| All ICMP-Verkehr Gesamter IP-Verkehr W2K to Zywall | Passt alle ICMP-Pakete zwisc Passt alle IP-Pakete von dies | Bearbeiten Entfernen |
| | | |
| | | |
| | < Zurück Weite | Abbrechen |

| Sicherheitsregel-Assistent | | ? × |
|---|--|--------------------------------------|
| Filteraktion Wählen Sie die Filteraktion für dies | e Sicherheitsregel. | |
| Klicken Sie auf "Hinzufügen", um e folgenden Liste den Anforderungen um eine Filteraktion Schritt für Schri | eine neue Filteraktion zu erstellen, (1 entspricht, Aktivieren Sie "Assiste itt zu erstellen, | wenn keine in der nt verwenden'', |
| Filteraktionen: | V | Assistent verwenden |
| Name | Beschreibung | Hinzufügen |
| IKE Sicherheit anfordern (optional) Sicherheit erforderlich Zulassen | Ungesicherte Kommunikation Ungesicherte Kommunikation Ungesicherte IP-Pakete durc | Bearbeiten Entfernen |
| | < Zurück Weite | er > Abbrechen |



| Eigenschaften von Zywall | | | <u>? ×</u> | | |
|---|---------|------------------|--------------------------|--|--|
| Regeln Allgemein | | | | | |
| Sicherheitsregeln für die Kommunikation mit anderen Computern | | | | | |
| IP-Sicherheitsregeln: | | | | | |
| IP-Filterliste | Filtera | Authentifizieru | Tunneleinstell | | |
| Zywall to W2k | IKE | Vorinstallierter | 213.3.123.66 | | |
| ₩2K to Zywall | IKE | Vorinstallierter | 195.246.70.100 | | |
| Oynamisch> | Stand | Kerberos | Keine | | |
| I Bearbe | iten | Entfernen | ► Assistent verwenden | | |
| Schließen Abbrechen | | | | | |

| 🔹 Lokale Sicherheitseinstellungen | | | | | |
|---|--------------------------|------------------------------|-----------------------|--|--|
| Vorgang Ansicht $] \Leftrightarrow \Rightarrow \boxed{1}$ $\boxed{1}$ $\boxed{2}$ $\boxed{2}$ $\boxed{2}$ $\boxed{2}$ $\boxed{2}$ $\boxed{2}$ $\boxed{2}$ | | | | | |
| Struktur | Name 🛆 | Beschreibung | Richtlinie zugewiesen | | |
| Sicherheitseinstellungen | 🛛 🖾 Client (nur Antwort) | Normale (ungesicherte) Kom | Nein | | |
| E G Kontorichtlinien | Server (Sicherheit anf | Sicherheit ist für den gesam | Nein | | |
| 🗄 📲 📴 Lokale Richtlinien | Sicherer Server (Siche | Sicherheit ist für den gesam | Nein | | |
| Richtlinien öffentlicher Schlüssel Reg. IP-Sicherheitsrichtlinien auf lokalem Computer | Zuweisen | | Nein | | |
| - | Alle Tasks | • | | | |
| | Löschen | | | | |
| | Umbenennen | | | | |
| | Eigenschaften | | | | |
| | Hilfedatei anzeigen | _ | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| Weist eine Richtlinie zu und versucht diese zu aktivieren. | | | | | |

| 🛃 Lokale Sicherheitseinstellungen | | | | | |
|---------------------------------------|--|--|-----------------------|--|--|
| Vorgang Ansicht ← → 🔁 🖬 🖗 🛱 🔡 🏦 | | | | | |
| Struktur | Name 🛆 | Beschreibung | Richtlinie zugewiesen | | |
| Sicherheitseinstellungen | Client (nur Antwort) Server (Sicherheit anf Sicherer Server (Siche Zywall | Normale (ungesicherte) Kom Sicherheit ist für den gesam Sicherheit ist für den gesam | Nein Nein Ja | | |
| | , | | | | |

TEST: Ping 192.168.1.1

| 🖾 C:\WINNT\System32\cmd.exe - ping 192.168.1.1 -t | |
|--|--|
| IP-Sicherheit wird verhandelt. | |
| IP-Sichawheit wird verhandelt. | |
| IP-Sichenheit wird verhandelt | |
| IP-Sicherheit wird verhandelt. | |
| Antwort von 192.168.1.1: Bytes=32 Zeit=100ms TTL=254 | |
| Antwort von 192.168.1.1: Bytes=32 Zeit=70ms TTL=254 | |
| Antwort von 192.168.1.1: Bytes=32 Zeit=20ms IIL=254 | |
| Antwort von 192.168.1.1: Bytes=32 Zeit=70ms IIL=254 | |
| Antwort von 192.168.1.1: Bytes=32 Zeit=70ms IIL=254 | |
| Antwort von 192.168.1.1: Bytes=32 Zeit=71ms IIL=254 | |
| Antwort von 192.168.1.1: Bytes=32 Zett=70ms IIL=254 | |
| HNTWOPT VON 172.168.1.1: Bytes=32 Zelt=70ms 11L=254 | |
| HILWOPE VON 172.168.1.1. Bytes-32 Zeit=70ms IIL=254 | |
| | |