

Konfigurieren eines standortübergreifenden VPN-Tunnels zwischen Routern der RV-Serie und Adaptive Security Appliances der Serie ASA 5500

Ziel

Sicherheit ist von entscheidender Bedeutung, um das geistige Eigentum eines Unternehmens zu schützen und gleichzeitig die Geschäftskontinuität zu gewährleisten und die Möglichkeit zu bieten, den Unternehmensarbeitsplatz auf Mitarbeiter auszuweiten, die jederzeit und überall Zugriff auf Unternehmensressourcen benötigen.

VPN-Sicherheitslösungen werden für kleine und mittlere Unternehmen immer wichtiger. Ein VPN ist ein privates Netzwerk, das innerhalb einer öffentlichen Netzwerkinfrastruktur, z. B. dem globalen Internet, aufgebaut ist. Ein VPN erweitert ein privates Netzwerk zwischen geografisch getrennten Bürostandorten. Es ermöglicht einem Host-Computer, Daten über öffentliche Netzwerke zu senden und zu empfangen, da diese mit allen Funktionen integraler Bestandteil des privaten Netzwerks waren. VPNs erhöhen die Sicherheit in einem verteilten Unternehmen und erleichtern es Mitarbeitern, von verschiedenen Standorten aus zu arbeiten, ohne das Netzwerk zu beeinträchtigen. Die Motivation für den Einsatz von VPN liegt in den Anforderungen zur "Virtualisierung" eines Teils der Unternehmenskommunikation und der Wirtschaftlichkeit der Kommunikation.

Es gibt verschiedene VPN-Topologien: Hub-and-Spoke, Point-to-Point und Full Mesh. Dieser Smart Tipp behandelt das standortübergreifende (Punkt-zu-Punkt) VPN, das eine internetbasierte Infrastruktur bereitstellt, um Netzwerkressourcen auf Außenstellen, Heimbüros und die Standorte von Geschäftspartnern auszuweiten. Der gesamte Datenverkehr zwischen Standorten wird mit dem IP Security (IPsec)-Protokoll verschlüsselt, und Netzwerkfunktionen wie Routing, Quality of Service (QoS) und Multicast-Unterstützung sind integriert.

Die Router der Cisco RV-Serie stellen robuste und einfach verwaltbare VPN-Lösungen für kostenbewusste kleine und mittlere Unternehmen bereit. Die Cisco Adaptive Security Appliances der Serie ASA 5500 ermöglichen ein ausgewogenes Verhältnis zwischen Sicherheit und Produktivität. Sie kombiniert die branchenweit am häufigsten eingesetzte Stateful Inspection-Firewall mit umfassenden Netzwerksicherheitsservices der nächsten Generation, darunter: Transparenz und präzise Kontrolle von Anwendungen und Mikroanwendungen, Web-Sicherheit, Intrusion Prevention Systems (IPS), hochsicherer Remote-Zugriff und andere.

In dieser Kurzreferenz wird ein Beispiel für das Design zur Einrichtung eines Site-to-Site-IPsec-VPNs zwischen Routern der RV-Serie und Adaptive Security Appliances der Serie ASA 5500 beschrieben. Außerdem werden Konfigurationsbeispiele aufgeführt.

Unterstützte Geräte

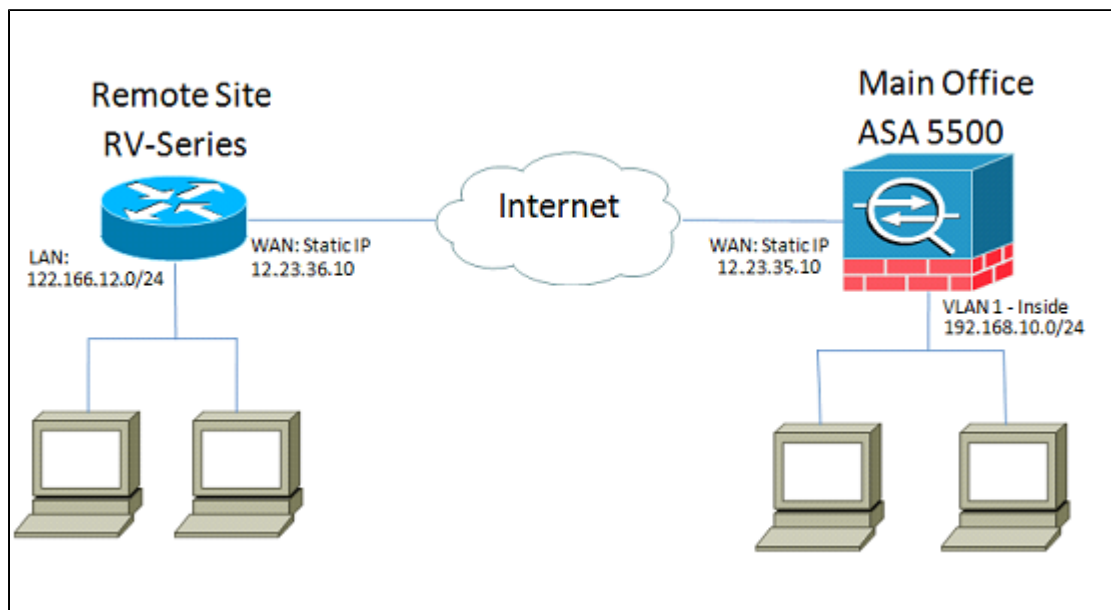
âf» Cisco VPN-Router der Serie RV0xx
â€¢ Cisco Adaptive Security Appliances der Serie ASA 5500

Software-Version

âf» 4.2.2.08 [Cisco VPN-Router der Serie RV0xx]

Vorkonfiguration

Das folgende Bild zeigt eine Beispielimplementierung eines standortübergreifenden VPN-Tunnels unter Verwendung eines Routers der RV-Serie (Remote-Standort) und einer ASA 5500 (Hauptniederlassung).



Mit dieser Konfiguration können ein Host im Remote-Standortnetzwerk 122.166.12.x und ein Host im VLAN 1 in der Hauptniederlassung sicher miteinander kommunizieren.

Wichtigste Funktionen

Internet Key Exchange (IKE)

Internet Key Exchange (IKE) ist das Protokoll, mit dem eine Sicherheitszuordnung (Security Association, SA) in der IPsec-Protokoll-Suite eingerichtet wird. IKE basiert auf dem Oakley-Protokoll und dem Internet Security Association and Key Management Protocol (ISAKMP) und verwendet einen Diffie-Hellman-Schlüsselaustausch, um einen gemeinsamen Sitzungsschlüssel einzurichten, von dem kryptografische Schlüssel abgeleitet werden. Eine sichere Richtlinie für jeden Peer muss manuell verwaltet werden.

Internet-Protokollsicherheit (IPSec)

IPsec verwendet kryptografische Sicherheitsdienste, um die Kommunikation über IP-Netzwerke (Internet Protocol) zu schützen. IPsec unterstützt Peer-Authentifizierung auf Netzwerkebene, Datenursprungsauthentifizierung, Datenintegrität, Datenvertraulichkeit (Verschlüsselung) und Wiedergabeschutz. IPsec umfasst viele Komponententechnologien und Verschlüsselungsmethoden. Der Betrieb von IPsec lässt sich jedoch in fünf Hauptschritte unterteilen:

Schritt 1: "Interessanter Datenverkehr" initiiert den IPsec-Prozess - Datenverkehr gilt als interessant, wenn die in den IPsec-Peers konfigurierte IPsec-Sicherheitsrichtlinie den IKE-Prozess startet.

Schritt 2: IKE Phase 1 - IKE authentifiziert IPsec-Peers und handelt in dieser Phase IKE-SAs aus. Dadurch wird in Phase 2 ein sicherer Kanal für die Aushandlung von IPsec-SAs eingerichtet.

Schritt 3: IKE Phase 2 - IKE handelt IPsec-SA-Parameter aus und richtet übereinstimmende IPsec-SAs in den Peers ein.

Schritt 4: Datenübertragung - Die Daten werden zwischen IPsec-Peers übertragen, basierend auf den

IPSec-Parametern und -Schlüsseln, die in der SA-Datenbank gespeichert sind.

Schritt 5: IPSec-Tunnelabschluss - IPSec-SAs werden durch Löschung oder durch Zeitüberschreitung beendet.

ISAKMP

Internet Security Association und Key Management Protocol (ISAKMP) werden verwendet, um den Tunnel zwischen den beiden Endpunkten auszuhandeln. Es definiert die Verfahren für Authentifizierung, Kommunikation und Schlüsselgenerierung und wird vom IKE-Protokoll verwendet, um Verschlüsselungsschlüssel auszutauschen und die sichere Verbindung herzustellen.

Design-Tipps

VPN-Topologie - Bei einem Site-to-Site-VPN wird zwischen jedem Standort und jedem anderen Standort ein sicherer IPsec-Tunnel konfiguriert. Eine Topologie mit mehreren Standorten wird in der Regel als ein vollständiges Netz aus Site-to-Site-VPN-Tunneln implementiert (d. h. jeder Standort verfügt über Tunnel zu jedem anderen Standort). Wenn keine Kommunikation zwischen Außenstellen erforderlich ist, wird eine Hub-Spoke-VPN-Topologie verwendet, um die Anzahl der VPN-Tunnel zu reduzieren (d. h., jeder Standort richtet einen VPN-Tunnel nur zur Hauptniederlassung ein).

WAN-IP-Adressierung und DDNS - Der VPN-Tunnel muss zwischen zwei öffentlichen IP-Adressen erstellt werden. Wenn die WAN-Router statische IP-Adressen vom Internet Service Provider (ISP) erhalten, kann der VPN-Tunnel direkt mithilfe statischer öffentlicher IP-Adressen implementiert werden. Die meisten kleinen Unternehmen nutzen jedoch kosteneffiziente Breitband-Internetdienste wie DSL- oder Kabelmodems und erhalten dynamische IP-Adressen von ihren ISPs. In solchen Fällen kann DDNS verwendet werden, um die dynamische IP-Adresse einem vollqualifizierten Domännennamen (Fully Qualified Domain Name, FQDN) zuzuordnen.

LAN-IP-Adressierung - Die privaten LAN-IP-Netzwerkadressen der einzelnen Standorte dürfen sich nicht überschneiden. Die standardmäßige LAN-IP-Netzwerkadresse an jedem Remote-Standort sollte immer geändert werden.

VPN-Authentifizierung - Das IKE-Protokoll dient zur Authentifizierung von VPN-Peers bei der Einrichtung eines VPN-Tunnels. Es gibt verschiedene IKE-Authentifizierungsmethoden, und der vorinstallierte Schlüssel ist die bequemste Methode. Cisco empfiehlt, einen starken vorinstallierten Schlüssel zu verwenden.

VPN-Verschlüsselung - Um die Vertraulichkeit der über das VPN übertragenen Daten sicherzustellen, werden Verschlüsselungsalgorithmen verwendet, um die Nutzlast von IP-Paketen zu verschlüsseln. DES, 3DES und AES sind drei gängige Verschlüsselungsstandards. AES gilt im Vergleich zu DES und 3DES als die sicherste Variante. Cisco empfiehlt dringend die Verwendung von AES-128-Bit oder höher (z. B. AES-192 und AES-256). Je stärker der Verschlüsselungsalgorithmus jedoch ist, desto mehr Verarbeitungsressourcen sind erforderlich.

Tipps zur Konfiguration

Checkliste vor der Konfiguration

Schritt 1: Stellen Sie sicher, dass die ASA und der RV-Router beide mit dem Internet-Gateway (dem ISP-Router oder -Modem) verbunden sind.

Schritt 2: Schalten Sie den Cisco RV-Router ein, und verbinden Sie dann die internen PCs, Server und andere IP-Geräte mit dem LAN-Switch oder den Switch-Ports am RV-Router.

Schritt 3: Führen Sie den gleichen Vorgang für das Netzwerk hinter der ASA aus. Schritt 4: Stellen Sie sicher, dass die LAN-IP-Netzwerkadressen an jedem Standort konfiguriert sind und sich in unterschiedlichen Subnetzen befinden. In diesem Beispiel wird für das LAN der Hauptniederlassung 192.168.10.0/24, and, für das LAN der Außenstelle 122.166.12.0/24 verwendet.

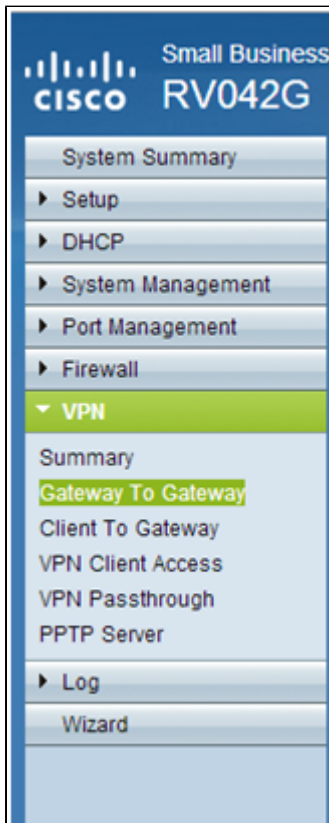
Schritt 4: Stellen Sie sicher, dass die lokalen PCs und Server miteinander und mit dem Router kommunizieren können.

Identifizieren der WAN-Verbindung

Sie müssen wissen, ob Ihr ISP eine dynamische IP-Adresse übergibt oder ob Sie eine statische IP-Adresse erhalten haben. Normalerweise erhält der ISP eine dynamische IP, aber Sie müssen dies bestätigen, um die Konfiguration abzuschließen.

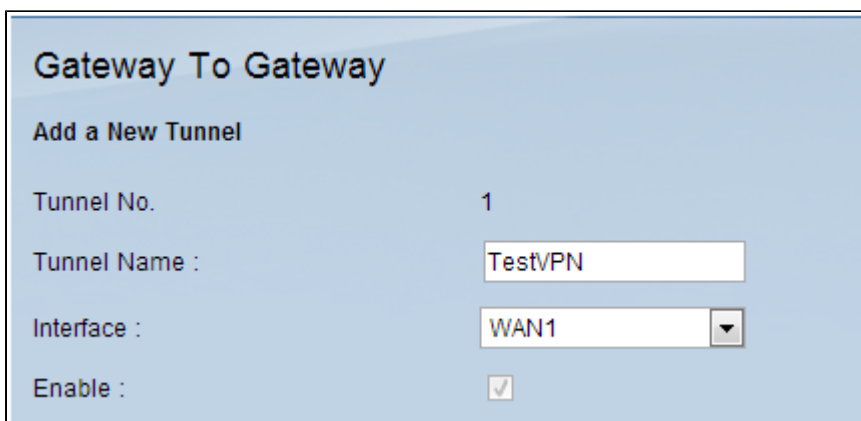
Konfigurieren des RV042G in der Außenstelle

Schritt 1: Melden Sie sich bei der Webbenutzeroberfläche an, und gehen Sie zum Abschnitt **VPN > Gateway to Gateway**. Da eine LAN-zu-LAN-Verbindung hinzugefügt wird, sind die Endpunkte das Gateway jedes Netzwerks.

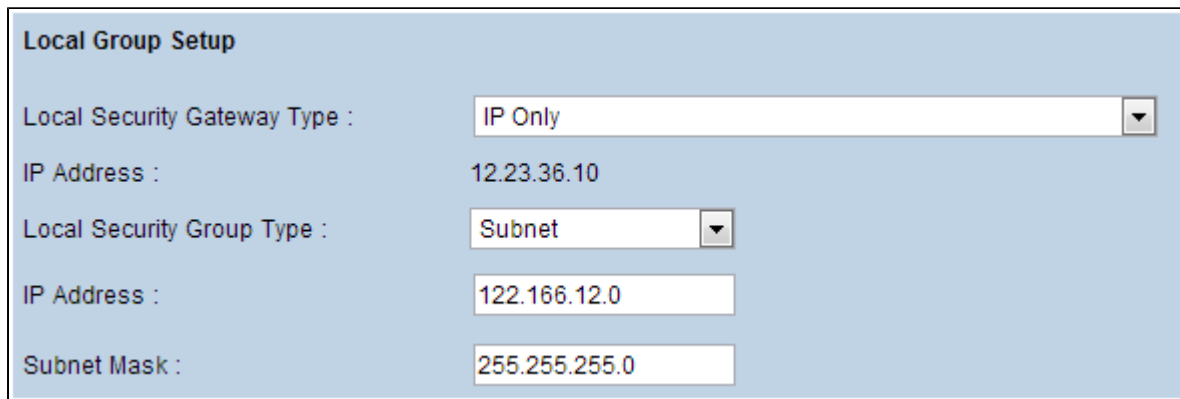


Schritt 2: Konfigurieren der lokalen und Remote-Endpunkte auf dem Router

a) Konfigurieren Sie den Tunnelnamen so, dass er von allen anderen Tunneln, die Sie möglicherweise bereits konfiguriert haben, erkannt wird.

The image shows the 'Gateway To Gateway' configuration page. The title is 'Gateway To Gateway'. Below the title is the section 'Add a New Tunnel'. There are four configuration fields: 'Tunnel No.' with the value '1', 'Tunnel Name' with the value 'TestVPN', 'Interface' with a dropdown menu showing 'WAN1', and 'Enable' with a checked checkbox.

b) Durch das Setup lokaler Gruppen werden die lokalen Hosts konfiguriert, die im VPN-Tunnel zugelassen werden sollen. Stellen Sie sicher, dass Sie über das richtige Subnetz und die richtige Maske für das Netzwerk verfügen, das Sie über den Tunnel zulassen möchten.



Local Group Setup

Local Security Gateway Type : IP Only

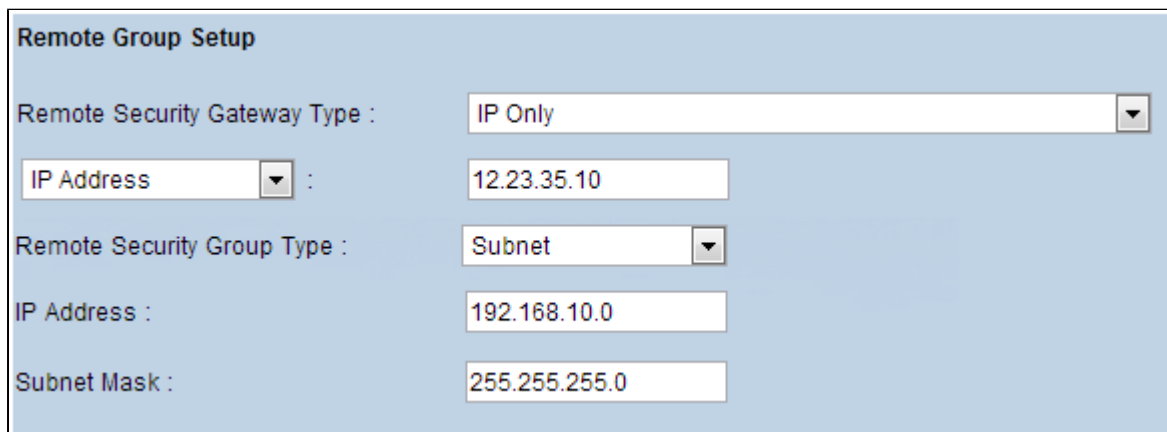
IP Address : 12.23.36.10

Local Security Group Type : Subnet

IP Address : 122.166.12.0

Subnet Mask : 255.255.255.0

c) Das Remote-Gruppen-Setup konfiguriert den Remote-Endpunkt- und Netzwerkverkehr, nach dem der Router sucht. Geben Sie die statische IP-Adresse des Remote-Gateways ein, um die Verbindung im IP-Adressfeld des Gateways herzustellen. Geben Sie dann das Subnetz ein, das auf dem VPN vom Remote-Standort (dem Hauptniederlassungs-LAN) zugelassen ist.



Remote Group Setup

Remote Security Gateway Type : IP Only

IP Address : 12.23.35.10

Remote Security Group Type : Subnet

IP Address : 192.168.10.0

Subnet Mask : 255.255.255.0

Schritt 3: Konfigurieren der Tunneleinstellungen

a) Sie möchten einen vorinstallierten Schlüssel konfigurieren, um optimale Ergebnisse zu erzielen.

Phase 1 und Phase 2 sind unterschiedliche Authentifizierungsphasen, Phase 1 erstellt den Anfangstunnel und beginnt mit der Aushandlung, und Phase 2 schließt die Aushandlung des Verschlüsselungsschlüssels ab und schützt die Datenübertragung, sobald der Tunnel eingerichtet ist.

b) Die DH-Gruppe entspricht der Crypto-ISAKMP-Richtliniengruppe auf der ASA, die im nächsten Abschnitt angezeigt wird. Auf ASA-Geräten ist der Standard "Group 2", und neuere Versionen von ASA-Code erfordern mindestens "DH Group 2". Der Nachteil besteht darin, dass das Bit höher ist und daher mehr CPU-Zeit benötigt.

c) Die Phase 1-Verschlüsselung definiert den verwendeten Verschlüsselungsalgorithmus. Die Standardeinstellung auf der RV-Serie ist DES, die Standardeinstellung auf der ASA ist jedoch 3DES. Hierbei handelt es sich jedoch um ältere Standards, die in der aktuellen Implementierung nicht effizient sind. Die AES-Verschlüsselung ist schneller und sicherer. Cisco empfiehlt für optimale Ergebnisse mindestens AES-128 (oder einfach AES).

d) Bei der Authentifizierung in Phase 1 wird die Paketintegrität überprüft. Die Optionen sind SHA-1 und MD5, und beide sollten funktionieren, da sie ähnliche Ergebnisse liefern.

Die Konfiguration von Phase 2 folgt denselben Regeln wie Phase 1. Beachten Sie beim Konfigurieren der IPSec-Einstellungen, dass die Einstellungen auf der ASA mit denen auf dem RV042G ÜBEREINSTIMMEN müssen. Bei Abweichungen können die Geräte den Verschlüsselungsschlüssel nicht aushandeln, und die Verbindung schlägt fehl.

Hinweis: Speichern Sie die Einstellungen, bevor Sie diese Seite verlassen!

| IPSec Setup | |
|---------------------------|--------------------------|
| Keying Mode : | IKE with Preshared key |
| Phase 1 DH Group : | Group 2 - 1024 bit |
| Phase 1 Encryption : | AES-128 |
| Phase 1 Authentication : | SHA1 |
| Phase 1 SA Life Time : | 28800 seconds |
| Perfect Forward Secrecy : | <input type="checkbox"/> |
| Phase 2 DH Group : | Group 2 - 1024 bit |
| Phase 2 Encryption : | AES-128 |
| Phase 2 Authentication : | SHA1 |
| Phase 2 SA Life Time : | 28800 seconds |
| Preshared Key : | c12c0VPn3x4mPL3 |

Konfigurieren der ASA 5500 in der Hauptniederlassung (CLI)

Hinweis: Stellen Sie sicher, dass Sie den Befehl "write mem" häufig verwenden, um Konfigurationsverluste zu vermeiden. Zunächst einmal sind dies die Schnittstellen, die wir auf der ASA konfiguriert haben. Ihre Konfiguration kann von der Ihren abweichen. Ändern Sie deshalb die Konfiguration entsprechend.

```
interface Vlan1
 nameif inside
 security-level 100
 ip address 192.168.10.1 255.255.255.0
!
interface Vlan10
 nameif outside
 security-level 0
 ip address 12.23.35.10 255.255.255.0
```

Schritt 1: Konfigurieren der Verschlüsselungsverwaltung (ISAKMP)

Der erste Schritt besteht in der Einrichtung der ISAKMP-Richtlinie, die verwendet wird, um die Verschlüsselung des Tunnels auszuhandeln. Diese Konfiguration sollte auf beiden Endgeräten IDENTISCH sein. Hier konfigurieren Sie die Verschlüsselungseinstellungen so, dass sie mit Phase 1 aus der RV-Konfiguration übereinstimmen.

```

ASA5505(config)# crypto isakmp policy 1
ASA5505(config-isakmp-policy)# authentication pre-share
ASA5505(config-isakmp-policy)# encryption aes
ASA5505(config-isakmp-policy)# hash sha
ASA5505(config-isakmp-policy)# group 2
ASA5505(config-isakmp-policy)# lifetime 28800
ASA5505(config-isakmp-policy)# exit
ASA5505(config)# █

```

Schritt 2: Datenverkehrsauswahl

Dies entspricht der lokalen und Remote-Sicherheitsgruppe auf dem RV042G. Auf der ASA verwenden wir Zugriffslisten, um zu definieren, was das Netzwerk als "interessanten Datenverkehr" für das VPN betrachtet.

Konfigurieren Sie zunächst die Netzwerkobjekte für den Remote-Standort und den lokalen Standort:

```

object network insidenet
  subnet 192.168.10.0 255.255.255.0
object network rsite
  subnet 122.166.12.0 255.255.255.0

```

Konfigurieren Sie dann die Zugriffsliste so, dass diese Objekte verwendet werden:

```

access-list vpn extended permit ip object insidenet object rsite

```

Alternativ können Sie die Subnetze selbst verwenden, in größeren Implementierungen ist es jedoch einfacher, Objekte und Objektgruppen zu verwenden.

Schritt 3: IPsec-Tunnelkonfiguration (Phase-2-Authentifizierung)

Hier konfigurieren Sie den "Transform Set" und die Tunnelgruppe, die die Phase-2-Authentifizierung einrichten wird. Wenn Sie Phase-2 so einrichten, dass sie sich von Phase-1 unterscheidet, haben Sie einen anderen Transformationssatz. Hier definiert esp-aes die Verschlüsselung und esp-sha-hmac den Hash.

Mit dem Befehl tunnel-group werden die verbindungs-spezifischen Tunnelinformationen konfiguriert, z. B. der vorinstallierte Schlüssel. Verwenden Sie die öffentliche IP-Adresse des Remote-Peers als Namen der Tunnel-Gruppe.

```

ASA5505(config)# crypto ipsec transform-set asarv esp-aes esp-sha-hmac
ASA5505(config)# tunnel-group 12.23.36.10 type ipsec-l2l
ASA5505(config)# tunnel-group 12.23.36.10 ipsec-attributes
ASA5505(config-tunnel-ipsec)# pre-shared-key c12c0VPn3x4mPL3
ASA5505(config-tunnel-ipsec)# exit
ASA5505(config)# █

```

Schritt 4: Konfiguration der Crypto Map

Jetzt müssen wir die Phase-1- und Phase-2-Konfiguration auf eine "Crypto Map" anwenden, die es der ASA ermöglicht, das VPN einzurichten und den richtigen Datenverkehr zu senden. Stellen Sie sich vor, dies würde die einzelnen Teile des VPN miteinander verbinden.

```

ASA5505(config)# crypto map asarv 1 match address vpn
ASA5505(config)# crypto map asarv 1 set peer 12.23.36.10
ASA5505(config)# crypto map asarv 1 set transform-set asarv
ASA5505(config)# crypto map asarv interface outside
ASA5505(config)# █

```

Schritt 5: Überprüfung des VPN-Status

Überprüfen Sie abschließend die Endgeräte, um sicherzustellen, dass die VPN-Verbindung einwandfrei funktioniert. Die Verbindung wird nicht von alleine hergestellt. Sie müssen Datenverkehr weiterleiten, damit die ASA sie erkennen und versuchen kann, die Verbindung herzustellen. Verwenden Sie auf der ASA den Befehl "show crypto isakmpsa", um den Status anzuzeigen.

```
ASA5505(config)# show crypto isakmp sa

Active SA: 1
Rekey SA: 0 (A tunnel will report 1 Active and 1 Rekey SA during rekey)
Total IKE SA: 1

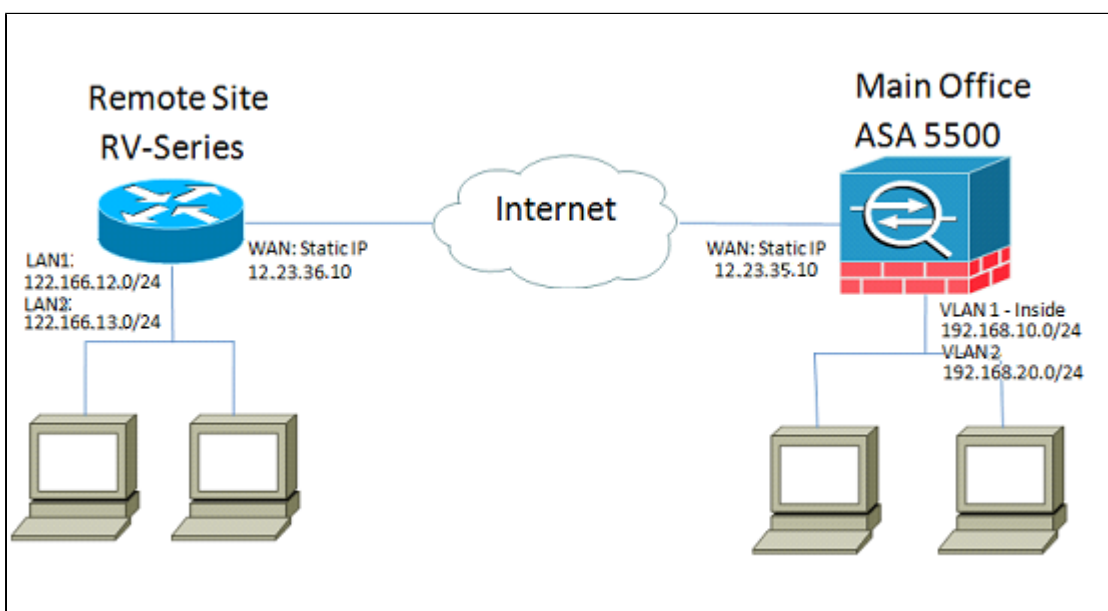
1 IKE Peer: 12.23.36.10
  Type    : L2L                Role    : responder
  Rekey   : no                 State   : MM_ACTIVE
ASA5505(config)#
```

Gehen Sie auf dem RV42G zur Seite **VPN > Summary (VPN > Zusammenfassung)**, und überprüfen Sie den Status.

| No. | Name | Status | Phase2 Enc/Auth/Grp | Local Group | Remote Group | Remote Gateway | Tunnel Test | Config. |
|-----|---------|-----------|---------------------|-------------------------------|-------------------------------|----------------|-------------|---------|
| 1 | TestVPN | Connected | AES/SHA1 | 122.166.12.0 255.255.255.0 | 192.168.10.0 255.255.255.0 | 12.23.35.10 | Disconnect | |

Alternativszenario: Mehrere Subnetze im Netzwerk

Keine Panik. Dies mag beim Einrichten des Netzwerks wie ein überwältigend komplizierter Prozess erscheinen, aber Sie haben den obigen Teil bereits erledigt. Die Konfiguration des VPNs für mehrere Subnetze erfordert eine zusätzliche Konfiguration, ist jedoch sehr komplex (es sei denn, Ihr Subnetzschemata ist umfangreich). Im vorliegenden Beispiel werden an jedem Standort zwei Subnetze verwendet. Die aktualisierte Netzwerktopologie ist sehr ähnlich:



Konfigurieren des RV042G

Zunächst wird der RV042G konfiguriert. Der RV042G kann nicht mehrere Subnetze über einen Tunnel konfigurieren. Aus diesem Grund müssen wir einen zusätzlichen Eintrag für das neue Subnetz hinzufügen. In diesem Abschnitt wird nur die VPN-Konfiguration für mehrere Subnetze behandelt, keine zusätzliche Setup-Konfiguration für diese Subnetze.

Schritt 1: Konfigurieren des ersten Tunnels

Wir verwenden für jeden Tunnel dieselbe Konfiguration wie für das Beispiel mit einem Subnetz. Sie können dies wie zuvor konfigurieren, indem Sie **VPN > Gateway to Gateway** aufrufen und einen neuen Tunnel hinzufügen. Wenn Sie einen vorhandenen Tunnel verwenden, wechseln Sie zur Seite **VPN > Zusammenfassung**, und bearbeiten Sie den vorhandenen Tunnel.

a) Konfigurieren Sie den Tunnelnamen, ändern Sie ihn jedoch, da mehrere Änderungen am Namen vorgenommen werden, um ihn beschreibend zu machen.

Gateway To Gateway

Add a New Tunnel

Tunnel No. 1

Tunnel Name :

Interface : ▼

Enable :

b) Als Nächstes konfigurieren Sie die lokale Gruppe wie zuvor. Konfigurieren Sie dies nur für EINES der Subnetze, auf die zugegriffen werden muss. Es gibt einen Tunnelleintrag für 122.166.12.x und einen weiteren für das Subnetz 122.166.13.x.

Local Group Setup

Local Security Gateway Type : ▼

IP Address : 12.23.36.10

Local Security Group Type : ▼

IP Address :

Subnet Mask :

c) Konfigurieren Sie nun den Remote-Standort, erneut mit dem gleichen Verfahren wie oben.

Remote Group Setup

Remote Security Gateway Type : IP Only

IP Address : 12.23.35.10

Remote Security Group Type : Subnet

IP Address : 192.168.10.0

Subnet Mask : 255.255.255.0

d) Konfigurieren Sie abschließend die Verschlüsselungseinstellungen. Denken Sie daran, diese Einstellungen für beide zu konfigurierenden Tunnel gleich zu halten.

IPSec Setup

Keying Mode : IKE with Preshared key

Phase 1 DH Group : Group 2 - 1024 bit

Phase 1 Encryption : AES-128

Phase 1 Authentication : SHA1

Phase 1 SA Life Time : 28800 seconds

Perfect Forward Secrecy :

Phase 2 DH Group : Group 2 - 1024 bit

Phase 2 Encryption : AES-128

Phase 2 Authentication : SHA1

Phase 2 SA Life Time : 28800 seconds

Preshared Key : c12c0VPn3x4mPL3

Schritt 2: Konfigurieren des zweiten Tunnels

Nachdem Subnetz 1 für den VPN-Tunnel konfiguriert wurde, müssen wir zu **VPN > Gateway to Gateway** wechseln und einen zweiten Tunnel hinzufügen. Dieser zweite Eintrag wird im Wesentlichen wie der erste konfiguriert, jedoch mit den sekundären Subnetzen von jedem Standort.

a) Stellen Sie sicher, dass Sie ihm einen besonderen Namen geben, damit Sie wissen, welche Verbindung es ist.

Gateway To Gateway

Add a New Tunnel

| | |
|---------------|-----------------------------------------|
| Tunnel No. | 2 |
| Tunnel Name : | <input type="text" value="VPNsubnet2"/> |
| Interface : | <input type="text" value="WAN1"/> |
| Enable : | <input checked="" type="checkbox"/> |

b) Verwenden Sie das zweite Subnetz als Gruppe "Lokale Sicherheit".

Local Group Setup

| | |
|-------------------------------|--------------------------------------------|
| Local Security Gateway Type : | <input type="text" value="IP Only"/> |
| IP Address : | 12.23.36.10 |
| Local Security Group Type : | <input type="text" value="Subnet"/> |
| IP Address : | <input type="text" value="122.166.13.0"/> |
| Subnet Mask : | <input type="text" value="255.255.255.0"/> |

c) Verwenden Sie das zweite Remote-Subnetz als die Gruppe "Remote-Sicherheit".

Remote Group Setup

| | |
|-------------------------------------------|--------------------------------------------|
| Remote Security Gateway Type : | <input type="text" value="IP Only"/> |
| <input type="text" value="IP Address"/> : | <input type="text" value="12.23.35.10"/> |
| Remote Security Group Type : | <input type="text" value="Subnet"/> |
| IP Address : | <input type="text" value="192.168.20.0"/> |
| Subnet Mask : | <input type="text" value="255.255.255.0"/> |

d) Konfigurieren Sie die Verschlüsselung für Phase 1 und 2 genauso wie für den ersten Tunnel.

| IPSec Setup | |
|---------------------------|--------------------------|
| Keying Mode : | IKE with Preshared key |
| Phase 1 DH Group : | Group 2 - 1024 bit |
| Phase 1 Encryption : | AES-128 |
| Phase 1 Authentication : | SHA1 |
| Phase 1 SA Life Time : | 28800 seconds |
| Perfect Forward Secrecy : | <input type="checkbox"/> |
| Phase 2 DH Group : | Group 2 - 1024 bit |
| Phase 2 Encryption : | AES-128 |
| Phase 2 Authentication : | SHA1 |
| Phase 2 SA Life Time : | 3600 seconds |
| Preshared Key : | c12c0VPn3x4mPL3 |

Konfigurieren der ASA

Nun ändern wir die Konfiguration auf der ASA. Diese Konfiguration ist unglaublich einfach. Sie können dieselbe Konfiguration wie oben verwenden, da hier alle Verschlüsselungseinstellungen verwendet werden, jedoch nur eine geringfügige Änderung erforderlich ist. Wir müssen zusätzlichen Datenverkehr als "interessant" markieren, damit er von der Firewall über das VPN gesendet werden kann. Da wir eine Zugriffsliste verwenden, um interessanten Datenverkehr zu identifizieren, müssen wir diese Zugriffsliste lediglich ändern.

Schritt 1: Löschen Sie zunächst die alte Zugriffsliste, damit wir die Objekte in der ASA ändern können. Verwenden Sie das Formular "no" (Nein) des Befehls, um Konfigurationen in der CLI zu entfernen.

Schritt 2: Nachdem die ACL entfernt wurde, sollen neue Objekte für die neuen Subnetze erstellt werden (vorausgesetzt, Sie haben diese Subnetze noch nicht eingerichtet). Wir wollen sie auch beschreibender gestalten.

Basierend auf unserer VLAN-Konfiguration unten:

```
interface Vlan1
 nameif inside
 security-level 100
 ip address 192.168.10.1 255.255.255.0
!
interface Vlan2
 nameif engineering
 security-level 100
 ip address 192.168.20.1 255.255.255.0
!
interface Vlan10
 nameif outside
 security-level 0
 ip address 12.23.35.10 255.255.255.0
!
```

Wir benötigen eine Objektgruppe für das interne Hauptnetzwerk (192.168.10.x) und das Engineering-Netzwerk (192.168.20.x). Konfigurieren Sie die Netzwerkobjekte wie folgt:

```
ASA5505(config)# show run object
object network ASAvlan1
 subnet 192.168.10.0 255.255.255.0
object network ASAvlan2
 subnet 192.168.20.0 255.255.255.0
object network RVvlan1
 subnet 122.166.12.0 255.255.255.0
object network RVvlan2
 subnet 122.166.13.0 255.255.255.0
```

Schritt 3: Nachdem die relevanten Netzwerkobjekte konfiguriert wurden, können wir die Zugriffsliste so konfigurieren, dass der entsprechende Datenverkehr mit Tags versehen wird. Sie sollten sicherstellen, dass Sie für beide Netzwerke hinter der ASA einen Zugriffslisteneintrag für beide Remote-Subnetze haben. Das Endergebnis sollte so aussehen.

```
ASA5505(config)# show run access-list
access-list vpn extended permit ip object ASAvlan1 object RVvlan1
access-list vpn extended permit ip object ASAvlan1 object RVvlan2
access-list vpn extended permit ip object ASAvlan2 object RVvlan1
access-list vpn extended permit ip object ASAvlan2 object RVvlan2
```

Schritt 4: Da wir nun die alte Zugriffsliste gelöscht haben, müssen wir sie mit dem gleichen Befehl wie zuvor erneut auf die Crypto Map anwenden:

```
ASA5505(config)# crypto map asarv 1 match address vpn
```

Verbindung überprüfen





Und das war's! Ihr Tunnel sollte jetzt betriebsbereit sein. Initiieren Sie die Verbindung, und überprüfen Sie den Status mithilfe des Befehls "show crypto isakmpsa" auf der ASA.

```
ASA5505(config)# show crypto isakmp sa

Active SA: 1
Rekey SA: 0 (A tunnel will report 1 Active and 1 Rekey SA during rekey)
Total IKE SA: 1

1 IKE Peer: 12.23.36.10
  Type    : L2L           Role    : responder
  Rekey   : no           State   : MM_ACTIVE
ASA5505(config)#
```

Auf der RV-Serie wird der Status auf der Seite "VPN > Summary" (VPN > Übersicht) angezeigt.

| No. | Name | Status | Phase2 Enc/Auth/Grp | Local Group | Remote Group | Remote Gateway | Tunnel Test | Config. |
|-----|------------|-----------|---------------------|-------------------------------|-------------------------------|----------------|-------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1 | VPNSubnet1 | Connected | AES/SHA1 | 122.166.12.0 255.255.255.0 | 192.168.10.0 255.255.255.0 | 12.23.35.10 | Disconnect |   |
| 2 | VPNsubnet2 | Connected | AES/SHA1 | 122.166.13.0 255.255.255.0 | 192.168.20.0 255.255.255.0 | 12.23.35.10 | Disconnect |   |

Add Page 1 of 1



Video zu diesem Artikel anzeigen ...

[Klicken Sie hier, um weitere Tech Talks von Cisco anzuzeigen.](#)

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.