VPN, dead peer detection und dynamische DSL-Zugänge

Immer wieder taucht im Zusammenhang dieser drei Begriffe die Frage auf, warum korrekt eingerichtet VPN Tunnel trotzdem nicht ordnungsgemäß wieder aufgebaut werden. Dazu muss man sich mit der Vorgehensweise beim Start von IPSec und der Zusammenarbeit mit dynamischen IP-Adressen, wie sie typischerweise bei Einwahlzugängen vergeben werden, beschäftigen.

Beim Start der VPN-Module wird zunächst einmal überprüft, ob der eigene Name eine IP-Adresse oder ein Domain-Name ist.

Im letzteren Fall wird durch eine DNS-Abfrage die IP-Adresse ermittelt. Ist die eigene (dynamische) IP-Adresse nicht identisch mit der durch Namensauflösung ermittelten IP kann IPSec nicht starten: es kann sich ja niemand zu diesem Host verbinden (ipsec__plutorun 022 "Name": we have no ipsecN interface for either end of this connection) und macht deshalb keinen Sinn. Die Gegenseite eines definierten Tunnels bekommt diese IP-Adresse auch nur durch eine DNS-Abfrage heraus und versucht dann zu einer "falschen" IP-Adresse zu verbinden. Bei einer statisch vergebenen IP-Adresse existiert diese Fehlermöglichkeit schon mal gar nicht.

Im zweiten Schritt werden die in der ipsec.conf hinterlegten Tunnelbeschreibungen ausgelesen und gestartet. Auch hier gilt: statische IP-Adressen der Tunnel-Partner sind unproblematisch. Steht in der ipsec.conf für einen gegebenen Tunnel ein Name in der Form partner.dyndns.org muss auch hier zuerst eine DNS-Abfrage Klarheit über dessen IP-Adresse erbringen.

Wenn bis hierher alles in Ordnung war, wird der Tunnel (einfach gesprochen) in Betrieb genommen und die Aushandlung der Sicherheitsparameter läuft durch - Tunnel steht!

Dead Peer Detection:

Sinn und Zweck der DPD (= dead peer detection) ist, einen Mechanismus bereitzustellen, der Aufschluss darüber gibt, ob der Partner eines VPN-Tunnels noch reagiert und wie im anderen Fall daraufhin zu verfahren ist. Andere Firewallhersteller kochen manchmal ihr eigenes Süppchen oder loten die Grenzen der DPD-Definition aus, so dass nicht immer eine Einigung zustande kommt. Und manche Firewalls unterstützen auch gar kein DPD. Um das herauszufinden, hilft nur das Lesen der Dokumentation. In solchen Fällen hilft dann nur das Abschalten von DPD auf dem IPCop.

Erste Voraussetzung ist, dass beide Seiten die DPD unterstützen müssen. Spielt da einer nicht mit, hat die DPD für beide Seiten keinen Wert. Der Tunnel kommt gar nicht erst zustande, wenn nur ein Partner DPD aktiviert hat.

Man denke sich folgendes Beispiel-Szenario:
Der VPN-Tunnel steht und ist funktionstüchtig, es gehen aber momentan keine Pakete über diese Verbindung. Zur Überprüfung, ob der Partner noch reagiert sind folgende Werte in der ipsec.conf ausschlaggebend, z.B.

a) dpddelay=30
b) dpdtimeout=120
c) dpdaction=hold

dpddelay=30 bedeutet, dass alle 30 Sekunden ein Paket zum Partner geschickt wird (R_U_THERE, was frei übersetzt "bist du noch da" bedeutet). Normalerweise schickt der Partner daraufhin ein Paket zurück (R_U_THERE_ACK, soll heissen: "ja, ich bin da"). Dann ist alles gut. Wenn aber die Antwort unterbleibt, wartet unsere Seite max. 120 Sekunden (=dpdtimeout) ob doch noch eine Bestätigung erfolgt. Wenn nicht, wird der Tunnel als abgebrochen betrachtet und alle damit zusammenhängenden Parameter (z.B. eroute, SA, etc.) verworfen (dpdaction=clear). Das ist sinnvoll wenn es sich z.B. um einen Roadwarrior handelt, bei dem die DSL-Verbindung abgebrochen ist. Geht man von der Annahme aus, dass die andere Seite sich nur temporär nicht meldet, setzt man dpdaction=hold. Das wiederum macht nur Sinn, wenn der Partner eine statische IP-Adresse besitzt. Eine dynamisch zugeordenete IP-Adresse des Partners wird sich mit hoher Wahrscheinlichkeit nach einer Neueinwahl geändert haben. Deshalb sollte für dynamische Adressen der Eintrag dpdaction=restart drinstehen.

Die o.a. Werte können für jede Verbindung einzeln geändert werden, um verschiedenen Rahmenbedingungen gerecht zu werden.

Zusammenfassend wird somit klar, dass jeder Partner eines Tunnels derselben Problematik unterworfen ist. Dreh- und Angelpunkt ist die Namensauflösung beim Start der IPSec-Module. Hat sich im Betrieb die IP-Adresse eines Partnes geändert, merkt IPSec davon zuerst mal nichts. Ausgenommen sind statische IP-Adressen. Aber die sind ja immer gleich und machen deshalb auch kein Problem.

Mein Lösungsansatz:

Es muß ein Skript her, das in regelmäßigen Abständen überprüft, ob sich eine der IP-Adressen der Tunnelpartner geändert hat. Ein solches Skript findet Ihr im Add-On „wmt“ unter diesem Link:

http://www.compass-host.de/ipcop/wmt-0.2.0.tar.gz

Funktionsweise des Skripts:

Zuerst werden die Tunnelinformationen ausgelesen (es werden nur Net-To-Net Verbindungen überwacht. Roadwarrior werden meiner Erfahrung nach zuverlässig über die DPD abgehandelt).

Für jede Verbindung ruft sich das Skript selbst nochmals auf und arbeitet in einer Endlosschleife alle 60 Sekunden die Überprüfung der IP-Adressen ab. Wird dabei eine geänderte IP-Adresse entdeckt (egal ob die eigene und/oder die des Partners), wird ein Neustart der betreffenden Verbindung ausgelöst (es erfolgt keine vollständige Neuinitialisierung des VPN! Nur die betreffende Verbindung wird neu gestartet). Im Protokoll erfolgt bei Entdeckung einer geänderten IP-Adresse ein entsprechender Eintrag, z.B.:

(Tunnelname) right IP mismatch: restarting connection...

Wer möchte, kann selbstverständlich die Variable CHECK_INTERVAL im Skript anpassen. Der Wert

CHECK_INTERVAL='60'

definiert, dass nach jeder Schleife 60 Sekunden bis zur nächsten Überprüfung gewartet wird. Wer den Wert z.B. auf 120 Sekunden erhöht, lässt die Verbindungen einmal alle 2 Minuten überprüfen. Da es nach einem Leitungsabbruch bei einem Partner 2-3 Minuten dauert, ehe der wieder online ist **und** seine dynamische IP-Adresse aktualisiert hat, sind 60 Sekunden meines Erachtens ein guter Wert.

Zur Erklärung betrachte ich im Folgenden dieses Beispiel:

Grün1 --- Cop1 --- Internet --- Cop2 --- Grün2

Voraussetzungen:
1. Der Tunnel wird aufgebaut und funktioniert
2. Nach einer Zwangstrennung wird der Tunnel nicht wieder aufgebaut
3. Mind. einer der beiden Partner besitzt eine dynamische IP-Adresse

Nehmen wir für dieses Beispiel weiter an, dass beide Cops über eine Einwahl per PPPoE mit dynamischen IP-Adressen verfügen. Im Web-GUI im Bereich VPN ist keine Startverzögerung eingetragen (Wert = 0). Auf beiden Cops ist eine Net2Net-Verbindung eingerichtet, die bei manuellem Start den Tunnel aufbaut bzw. aufbauen kann. Für beide Cops ist ein DNS-Name bei z.B. DYNDNS.ORG hinterlegt (Cop1: cop1.dyndns.org; Cop2: cop2.dyndns.org). Cop1 macht um 05:00 Uhr eine Neuverbindung, Cop2 um 05:30 Uhr.

Initialzustand:
Cop1 und Cop2 sind mit dem Internet verbunden und haben den VPN-Tunnel lt. Verbindungsbeschreibung aufgebaut. Die jeweilige IP-Adresse wurde bei DYNDNS.ORG erfolgreich synchronisiert.

Was kann passieren ?

1.) Cop1 verliert seine PPPoE-Verbindung und wählt neu ein.
2.) Cop2 verliert seine PPPoE-Verbindung und wählt neu ein.
3.) Zwangstrennung bei Cop1 am nächsten Tag um 05:00
4.) Zwangstrennung bei Cop2 am nächsten Tag um 05:30
5.) VPN-Tunnel bricht zusammen ohne dass die Verbindung ins Internet getrennt wurde

Fall 1:
Cop1 wählt sich neu ein und bekommt eine neue IP-Adresse. Danach wird versucht, die neue IP-Adresse bei DYNDNS.ORG zu aktualisieren. Das benötigt etwas Zeit, typischwerweise eine bis fünf Minuten. Aber auch höhere Werte sind bekannt. Beinahe gleichzeitig starten die IPSec-Module. Dabei wird die eigene rote IP-Adresse mit der bei DYNDNS.ORG hinterlegten IP-Adresse verglichen. Bei Übereinstimmung wird VPN gestartet. Ergibt der Vergleich keine Übereinstimmung, läuft zwar IPSec, es kann aber kein Interface gestartet werden. Das ist logisch, denn unter der hinterlegten IP-Adresse kann Cop1 nicht erreicht und deshalb auch nie ein Tunnel aufgebaut werden.

Schlussfolgerung: Es muss genügend Zeit vergehen, damit die neue IP-Adresse sicher mit der bei DYNDNS.ORG hinterlegten IP-Adresse übereinstimmt. Entweder räumt man durch Eintrag eines genügend hohen Werts für die Startverzögerung ausreichend Zeit ein, damit die

Aktualisierung stattfinden kann. Eine andere Möglichkeit besteht darin, durch Neustart der IPSec-Module ca. 15-30 Min. nach dem Neuverbinden ausreichend Zeit vergehen zu lassen.

Fall 2:
Exakt dasselbe Verfahren wie für Cop1.

Fall 3 und 4:
Im Prinzip dassselbe wie bei Fall 1 und Fall 2. Da aber an dieser Stelle der genaue Zeitpunkt der Trennung bekannt ist, kann man besser darauf reagieren. Am einfachsten lassen wir den IPSec-Modulen genügend Startzeit und setzten die Startverzögerung auf 300 Sekunden. Ich gehe i.d.R. noch einen Schritt weiter und starte per cron nach ca. 15-30 Min. alle IPSec-Module neu ("/etc/rc.d/ipsec restart").

Fall 5:
Am schwierigsten zu behandeln. Eigentlich ein klarer Fall für die DPD (dead peer detection). Da sich die IP-Adresse NICHT ändert, kommt der Tunnel ganz von alleine wieder zu Stande. Falls nicht, kann das auch das Add-On wmt nicht ändern. Für das Skript hat sich ja nichts verändert!

Jetzt nehme ich an, dass WMT installiert wurde. Wie geht WMT zur Überprüfung vor ?

Für jede Verbindung, die lt. /var/ipcop/vpn/config als aktiv zu betrachten ist, und die einen Net2Net-Tunnel beschreibt wird ein eigener Aufruf des Skript erzeugt. In einer Endlosschleife, die alle 2 Minuten eine Überprüfung durchführt, werden folgende Werte ermittelt:

a) Auslesen der aktiven Verbindungsdaten. Daraus lässt sich die IP-Adresse des linken und des rechten Cops ermittlen (jeweils NUR die rote IP-Adresse laut letzter Verbindung). War der betreffende Tunnel nicht aktiv, kann das Skript auch keinen Wert für die IP-Adressen ermitteln.

b) DNS-Namensauflösung für cop1.dyndns.org und cop2.dyndns.org.
Das ergibt ebenfalls 2 IP-Adressen.

Zuerst vegleicht das Skript, ob sich die eigene IP-Adresse geändert hat. Danach ob sich die IP-Adresse des Partners geändert hat. Und abschliessend, ob sich vielleicht beide IP-Adressen geändert haben. In jedem dieser 3 Fälle ist bei Übereinstimmung der Werte keine Aktion erforderlich. Bei Nichtübereinstimmung wird der betreffende Tunnel neu gestartet indem ein Aufruf an die IPSec-Module abgesetzt wird, der die Anweisung enthält, welcher Tunnel neu zu starten ist.

wmt kontrolliert nicht selbst die Tunnel, sondern teilt nur im Falle einer Änderung einer IP-Adresse den IPSec-Modulen mit, daß ein Neustart erforderlich ist!

Hinweis:
Wenn die IPCops nicht direkt am Internet angeschlossen sind – z.B. noch ein Router dazwischen geschaltet wird – kann WMT Änderungen der IP-Adressen nicht korrekt erkennen! Dies gilt umso mehr, da dann i.d.R. beim roten Interface eine statische, nicht öffentliche IP-Adresse verwendet wird und in der Verbindungsbeschreibung die richtige öffentliche IP-Adresse oder ein DNS-Name benutzt wird. Die Vergleichsprüfung führt dann immer zum Neustart der Verbindung.

Installation:

1. Download des Add-On unter http://www.compass-host.de/ipcop/wmt-0.2.0.tar.gz
2. Auf den Cop in ein Verzeichnis kopieren (z.B. mit WinSCP)
3. Auf der Console entpacken mit „tar xvzf wmt-0.2.0.tar.gz“
4. In das neu erstellte Verzeichnis wmt-0.2.0 wechseln
5. ./install aufrufen

Zum Abschluss im Web-GUI aktivieren.
Ein Neustart des Cops ist nicht erforderlich.

Deinstallation:

1. Auf der Console anmelden und in das Installationsverzeichnis wechseln
2. ./uninstall aufrufen

Manuelle Kontrolle:

Auf der Console anmelden. Folgende Befehle sind möglich:

Start wmt: /usr/local/bin/wmtctrl start
Stop wmt: /usr/local/bin/wmtctrl stop
Status wmt: /usr/local/bin/wmtctrl status

W(atch) M(y) T(unnels) hat als Weiterentwicklung des Skriptes vpn-watch.sh begonnen und ist jetzt zu einem eigenen Add-On geworden:

wmt 0.2.0

Funktion:
Das Add-On bindet sich in die Web-Oberfläche unter STATUS->WMT (WATCH MY TUNNELS) sowie unter LOGS->SYSTEM-LOGDATEIEN als Sektion WMT ein. Nach Aktivierung wird das Skript wmt.sh gestartet, das im Hintergrund alle Net2Net-Verbindungen auf Änderung der IP-Adresse überwacht und ggfs. einzelne VPN-Tunnel neu startet.

Weiterhin erfolgt ein Eintrag in die Datei /etc/rc.d/rc.local um den Start des Skriptes bei Systemstart zu ermöglichen. Beim Start des Skriptes wird geprüft, ob eine Aktivierung über das Web-GUI erfolgt ist. Ist das nicht der Fall beendet sich das Skript wieder. Sollten die IPSec-Module beim Start des Skripts noch nicht gestartet worden sein (s.a. Einstellung bei VPN: Verzögerung bevor VPN gestartet wird), wartet das Skript auf die IPSec-Module bevor die Subprozesse gestartet werden.

Zum Aktivieren des Skripts nach Installation ist in der Web-GUI im Bereich Status der Eintrag "WMT (WATCH MY TUNNELS) aufzurufen und das Häkchen bei "Skript aktiviert" zu setzen. Schaltfläche "Speichern" anklicken - das wars!

Die Statusseite aktualisiert sich selbstständig einmal pro Minute.

Pro Zeile wird der Name der Net2Net-Verbindung, die Anzahl vom Skript ausgelöster Neustarts der Verbindung sowie Datum und Uhrzeit des letzten Prüflaufs angezeigt (s.a. http://www.compass-host.de/ipcop/wmt.jpg). Zur Erinnerung: Host2Net-Verbindungen (Roadwarrior) werden vom Skript nicht erfasst und nicht überprüft.

Die Sektion WMT im Bereich LOGS->SYSTEM-LOGDATEIEN dient zur Anzeige der protokollierten Statusmeldungen des Skripts.

Zu guter Letzt:

Die bereitgestellte Software wird ohne jegliche ausdrückliche oder implizierte Garantie - so wie sie ist - angeboten. Eine Produkthaftung und/oder Zusicherung der Gebrauchstauglichkeit wird hiermit ausgeschlossen.

Nutzung der Software erfolgt auf eigene Gefahr!

Der Autor kann nicht für jedwede mögliche Beschädigung oder Schaden verantwortlich gemacht machen, die durch den Gebrauch oder die Fehlanwendung von dieser Software verursacht werden könnte.

Stand: 16-10-2007